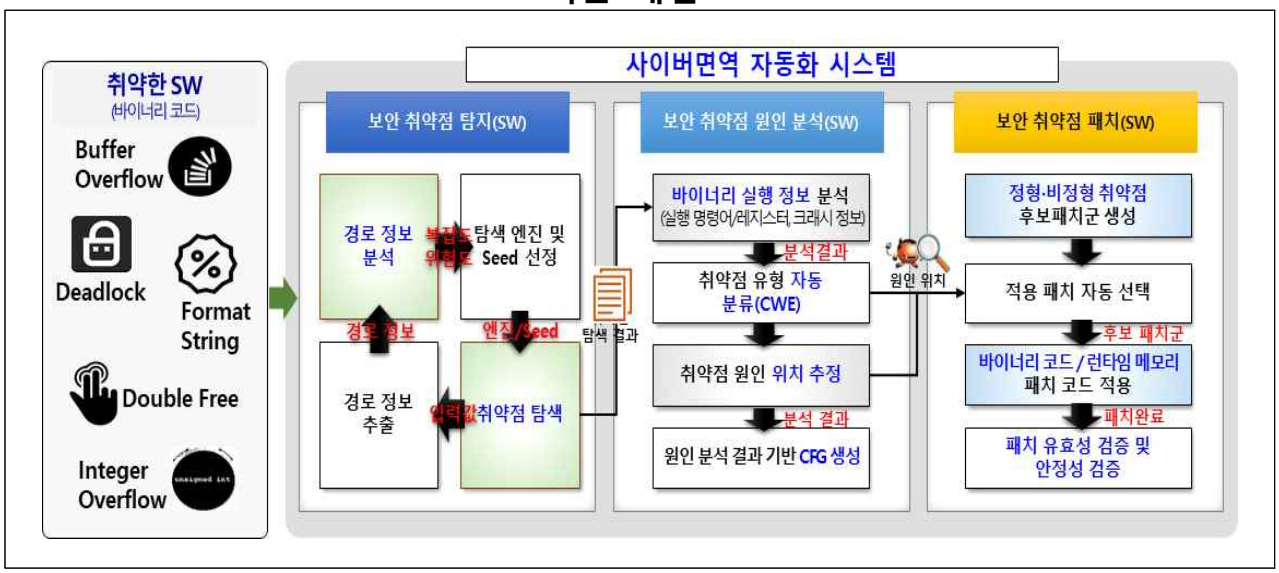
Ⅱ. 20년 기술이전 대상 목록

1 자기학습형 사이버면역 기술 ('17.3월 ~ '20.12월(4년))

□ 기술개요

o Legacy 시스템에 내재된 SW(리눅스 바이너리)의 보안 취약점을 자동으로 탐색하여 원인을 분석하고, 자동으로 바이너리 기반의 패치를 생성·적용하는 기술

< 기술 개념도 >



□ 기술의 특징 및 장점

o 하이브리드 퍼징 기반의 취약점, 기능오류 등 자동 탐색
- 바이너리의 위험도·복잡도를 분석하여 취약점 유발 효율 향상
(비교도구 대비 크래시 발생 유효 테스트케이스 2배 향상/총 20.16%)

o 정·동적 분석 정보 기반 취약점 유형(CWE) 및 발생 위치 분석(CWE 40종 식별)

o 취약점 별 바이너리 패치 생성·적용 및 유효성/안전성 검증

□ 활용 분야

① SW 개발·검증 단계의 취약점 분석 도구(탐지,원인분석)

② 유지보수가 종료된 운영 시스템의 취약점 관리(탐지, 원인분석, 패치)

□ 기술이전 내용 및 범위

구분	시스템	주요 내용
1	바이너리 보안 취약점 분석 시스템	o 바이너리를 대상으로 취약점을 탐색하고 취약점 유형 및 발생 원인을 분석(추적)하는 기술 o 세부 기술 구성 - 기술1 : 하이브리드 퍼징 - 기술2 : 바이너리 실행 흐름 변경 - 기술3 : 취약 바이너리 정적·동적 분석 - 기술4 : 보안 취약점 원인 위치 추적
2	바이너리 보안 취약점 자동 패치 시스템	o 바이너리 기반의 보안 취약점을 해결하기 위한 패치 선택 및 적용하는 기술 o 세부 기술 구성 - 기술1 : 바이너리 패치 엔진 관리 모듈 - 기술2 : 함수 기반 바이너리 취약점 패치 적용 모듈 - 기술3 : 명령어 기반 바이너리 취약점 패치 적용 모듈

□ 기술이전 문의

기술이전 담당	김태은 책임연구원(061-820-1273, rndts@kisa.or.kr)